

Title (en)  
A CRYPTOGRAPHIC METHOD

Title (de)  
VERSCHLÜSSELUNGSVERFAHREN

Title (fr)  
PROCEDE CRYPTOGRAPHIQUE

Publication  
**EP 0704124 A4 19990324 (EN)**

Application  
**EP 94902556 A 19931220**

Priority  
• AU 9300665 W 19931220  
• AU PL650292 A 19921222

Abstract (en)  
[origin: WO9415423A1] A cryptographic method including selecting secret keys  $p$  and  $q$ , being prime numbers greater than 3, selecting public parameters for a series of data values which belong to one of a plurality of pairs of groups whereby any one of the data values in one of the pairs of groups is recovered by performing an operation  $kN_i + 1$  times modulo  $n$  beginning with any one of the data values, where  $k$  is an integer,  $N_i$  is the order of the  $i$ -th pair of groups and  $n = p \cdot q$ , selecting a public encryption key  $e$  which is a factor of  $kN_i + 1$  for all  $i$ , and processing communications data as a member of one of the pairs of groups by performing the operation on the communications data, whereby the order  $N_i$  of the pair of groups  $i$  that the communications data belongs to can be determined on the basis of  $p$  and  $q$ , and a secret decryption key  $d_i$  can be determined using  $e \cdot d_i = kN_i + 1$ .

IPC 1-7  
**H04L 9/26**

IPC 8 full level  
**G09C 1/00** (2006.01); **G06F 7/72** (2006.01); **H04L 9/26** (2006.01); **H04L 9/30** (2006.01); **H04L 9/32** (2006.01)

CPC (source: EP US)  
**G06F 7/725** (2013.01 - EP US); **H04L 9/302** (2013.01 - EP US); **H04L 9/3066** (2013.01 - EP US); **H04L 9/3247** (2013.01 - EP US)

Citation (search report)  
• [XA] EP 0503119 A1 19920916 - OMNISEC AG [CH]  
• [A] KENJI KOYAMA ET AL: "ELLIPTIC CURVE CRYPTOSYSTEMS AND THEIR APPLICATIONS", IEICE TRANSACTIONS ON INFORMATION AND SYSTEMS, vol. E75 - D, no. 1, 1 January 1992 (1992-01-01), pages 50 - 57, XP000301174  
• See references of WO 9415423A1

Designated contracting state (EPC)  
AT BE CH DE DK ES FR GB GR IE IT LI LU MC NL PT SE

DOCDB simple family (publication)  
**WO 9415423 A1 19940707**; AU 5689594 A 19940719; AU 677269 B2 19970417; CA 2150683 A1 19940707; CA 2150683 C 19990907; EP 0704124 A1 19960403; EP 0704124 A4 19990324; JP H08504962 A 19960528; US 5627893 A 19970506

DOCDB simple family (application)  
**AU 9300665 W 19931220**; AU 5689594 A 19931220; CA 2150683 A 19931220; EP 94902556 A 19931220; JP 51460294 A 19931220; US 44681695 A 19950724